

An Examination of the ISACA Code of Professional Ethics.

David M. Cannon, Ph.D., CISA, CIA, CPA (Ohio), CCP

Assistant Professor

Department of Accounting and Taxation

Grand Valley State University

***West Michigan Chapter Meeting of the Information
Systems Audit and Control Association***

November 18, 2005

Ethics Codes

- Set of moral values and principles to guide and shape decisions and behavior
- Must be communicated to stakeholders
- Defines the desired collective behavior of profession
 - Who we are
 - What we stand for
- Defines the desired behavior of individual professionals

Ethics Codes describes obligations

- to society
- to employer
- to a client
- to colleagues and the profession

How are conflicts resolved between these obligations?

How do we know if we are making ethical decisions?

- The “mom test”
 - What would your mom say?
- The “I-team test”
 - Would the local TV or newspaper I-Team be interested in your decision(s)
- The “market test”
 - How would you feel about a major marketing initiative designed to publicize and promote your decision

from Boswoth and Kabay (2002) Computer Security Handbook, Wiley.

1. Members and ISACA certification holders shall:

Support the implementation of, and encourage compliance with, appropriate standard procedures and controls for information systems

Why do we care about encouraging compliance with IS standards?

- We're not talking about auditing standards here
- *What (or which) IS standards?*

Other Professional Standards

- Accounting, Engineering, Law, Medicine
 - Common body of knowledge
 - Generally accepted standards for practice of professions
 - » GAAP, GAAS, Model Accountancy Act, etc.
 - » IEEE, ASME, etc.
 - » ABA model rules
 - » Medical specialty standards of care
 - Standard educational requirements for professions

No comparable IT professional standards has been agreed upon

- IT practitioners come from diverse backgrounds
 - Formal education in information systems versus computer science
 - Fast food worker one day, “paper MCSE” the next
 - Self-taught in programming
- No generally accepted common body of knowledge
 - While organizations have adopted common body of knowledge (e.g., ICCP Core Exam, AIS Model Curriculum), none are universally accepted
- No generally accepted standards of practice

IT cultural resistance to standards, procedures and controls

- “restrains innovation and creativity”
- “gets in the way of getting things done”
- “who cares as long as it works”
- “standards are great, but not with this deadline”
- “we’ve always done it this way and there’s never been a problem”
- “I don’t see how this is value-added”

2. Members and ISACA certification holders shall:

Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices

Objectivity

- Auditor acts from a neutral perspective
- Auditor is free from bias
- Auditor deals only with verifiable facts

Due diligence and professional care

■ Due diligence

- *noun*: the effort that a reasonable person expends under the circumstances to avoid harm to other persons or their property

adapted from definition in Online Merriam-Webster's dictionary

■ Due professional care

- *noun*: the level of diligence which a prudent and competent individual that professes to exercise a special skill such as information systems auditing

from ISACA Audit Guideline 030.0202

Professional standards and best practices

■ Professional standards

- IS Auditing Standards
- Compliance with standards mandatory
- If adherence to standards impaired, IS auditor should consider withdrawing from engagement

from ISACA IS Auditing Standard Commentary

■ Best Practices

- ISACA IS Auditing Guidelines
- IS Auditing Procedures
- COBIT Framework
- NOT mandatory

3. Members and ISACA certification holders shall:

Serve in the interest of stakeholders in a lawful and honest manner, while maintaining standards of conduct and character, and not engage in acts discreditable to the profession

Maintaining standards of conduct and character

The IS auditor should

- maintain the highest degree of integrity and conduct
- not adopt any methods that could be seen as
 - » unlawful,
 - » unethical, or
 - » Unprofessional

from IS Auditing Standard 030

Acts discreditable to the profession

“catch all provision”

- any felony conviction
- commission of fraud
- conviction of any crime involving moral turpitude
- gross negligence in practice of IS auditing
- accepting bribes in the course of an audit
- etc.

4. Members and ISACA certification holders shall:

Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for benefit of or released to inappropriate parties.

Privacy versus confidentiality

- Privacy is about people
 - individual right to privacy
 - deals with accessing sensitive personal information about others
- Confidentiality is about data
 - obligation to protect existing sensitive data from access or inappropriate disclosure

Disclosure required by legal authority

- Subpoena, summons or court order
- Regulatory agencies
- Contractual obligations to disclose
- External auditor requests
- Legal advice should be sought prior to disclosing irregularities or illegal acts

5. Members and ISACA certification holders shall:

Maintain competency in their respective fields and agree to undertake only those activities which they can reasonably expect to complete with professional competence.

Maintain competency in respective field

- The IS auditor is primarily responsible for acquiring the required professional and technical skills and knowledge to carry out any assignment the IS auditor *agrees* to perform
- the auditor should decline an assignment that the auditor does not believe he/she is competent to perform or obtain the required technical skills and knowledge prior to carrying out the assignment
- Skills and knowledge vary with the role the auditor performs on the engagement

Maintain competency in respective field

- The IS auditor should continually monitor their skills and knowledge to maintain the acceptable level of competence
 - Competence should be evaluated periodically
 - The auditor should maintain competence through continuing professional education

Professional competence

- means that the IS auditor has the skills and knowledge of an individual that professes to have special skills in a particular area

6. Members and ISACA certification holders shall:

Inform appropriate parties of work performed; revealing all significant facts to them.

Reporting

- Management of audited area should have opportunity to review report in draft form
 - Managements comments should be included in final report
- If the IS auditor finds significant deficiencies in the control environment, the auditor should communicate these deficiencies to the audit committee or responsible authority

Among other things, all significant facts includes

- constraints placed on the auditor by the auditee
- impairment of auditor independence
- significant deficiencies in internal control
- management's disagreement with audit findings

7. Members and ISACA certification holders shall:

Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Professional education of stakeholders

- Awareness of information security issues is a general control
 - Good information security has hard costs, but soft benefits
 - Helps managers make informed decisions about dealing with risks

Violation of the Code of Professional Ethics

from Section 2.09 of ISACA bylaws

“ . . .the Board, acting in good faith, may, by a two-thirds vote of those present, terminate the membership of any member who in its judgment has violated the . . . Code of Ethics of the Association, or who has been guilty of conduct detrimental to the best interests of the Association . . .”



Questions?
Comments?
Discussion?